Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (previously presented) A method for defence against an attack made by means of differential power analysis, the method comprising:

randomizing at least one factor in a hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, wherein the factor is selected from the group consisting of:

the hyperelliptic curve; and
at least one element of the first group.

2. (previously presented) A method as claimed in claim 1, wherein bits of the operand to be processed or encoded in the hyperelliptic public key cryptosystem are represented by at least one co-efficient of the hyperelliptic curve.

3. (previously presented) A method as claimed in claim 1, wherein at least one scalar multiplication in a Jacobian variation of the hyperelliptic curve takes place in a second group different from the first group and isomorphic in relation to the first group, in particular selected at random.

4. (previously presented) A method as claimed in claim 3, further comprising:

transforming the Jacobian variation of the hyperelliptic curve, by means of at least one K-isomorphism, into the Jacobian variation of the transformed hyperelliptic curve;

multiplying the Jacobian variation of the transformed hyperelliptic curve with at least one scalar; and

transforming the Jacobian variation multiplied by the scalar of the transformed hyperelliptic curve by means of the depiction inverse to the depiction in Jacobian variations of the hyperelliptic curve multiplied by scalars, where the depiction corresponds to the transition from the first group to the second group and the inverse depiction corresponds to the transition from the second group to the first group.

5. (previously presented) A method as claimed in claim 1, further comprising:

depicting at least one reduced divisor with an associated polynomial pair as at least one quintuplet in projective co-ordinates, where $U(t)=t^2+U_1t/Z+U_0/Z$ and $V(t)=V_1t/Z+V_0/Z$;

randomly selecting at least one non-vanishing element from the field; and

converting the quintuplet by means of a selected element into a converted quintuplet.

6. (previously presented) A method as claimed in claim 1, further comprising:

depicting at least one reduced divisor with associated polynomial pair as at least one sextuplet a projective co-ordinates, where $U(t)=t^2+U_1t/Z_1^2+U_0/Z_1^2$ and $V(t)=V_1t/(Z_1^3Z^2)+V_0/(Z_1^3Z_2)$;

randomly selecting at least two non-vanishing elements from the field; and

converting the sextuplet by means of a selected elements into a converted sextuple.

7. (previously presented) A method as claimed in claim 1, further comprising implementing the method on a microprocessor of a smart card.

8. (previously presented) A microprocessor to implement instructions for defence against at least one attack made by means of differential power analysis in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, wherein the microprocessor is configured to randomize at least one factor selected from the group consisting of the hyperelliptic curve and at least one element of the first group.

9. (previously presented) A smart card, the smart card comprising at least one microprocessor as claimed in claim 8.

10. (previously presented) Use of a method as claimed in claim 1 in the defence against at least one attack made by means of differential power analysis on at least one hyperelliptic public key cryptosystem.

11. (previously presented) The method of claim 1, wherein randomizing at least one element of the first group comprises randomizing at least one reduced divisor.

12. (previously presented) The method of claim 1, wherein randomizing at least one element of the first group comprises randomizing at least one intermediate result of a scalar multiplication.

13. (previously presented) The method of claim 1, wherein bits of the operand to be processed and/or encoded in the hyperelliptic public key cryptosystem are represented by at least one base element of the cryptosystem, wherein the base element comprises at least one reduced divisor, at least one intermediate result of a scalar multiplication, or at least one of each of the reduced devisor and the intermediate result of the scalar multiplication.